Continuous Risk Management at NASA

Dr. Linda H. Rosenberg	Theodore Hammer	Albert Gallo
Unisys @ NASA GSFC SATC	NASA GSFC	Unisys @ NASA GSFC SATC
Bld 6 Code 300.1	Bld 6 Code 302	Bld 6 Code 300.1
Greenbelt, MD 20771	Greenbelt, MD 20771	Greenbelt, MD 20771
301-286-0087	301-286-7123	301-286-8012
Linda.Rosenberg@gsfc.nasa.gov	Thammer@pop300.gsfc.nasa.gov	agallo@mail.hst.nasa.gov

Abstract

NPG 7120.5A, "NASA Program and Project Management Processes and Requirements" enacted in April, 1998, requires that "The program or project manager shall apply risk management principles…" The Software Assurance Technology Center (SATC) at NASA GSFC has been tasked with the responsibility for developing and teaching a systems level course for risk management that provides information on how to comply with this edict. This risk management structure of functions has been taught to projects at all NASA Centers and is being successfully implemented on many projects. The course was developed in conjunction with the Software Engineering Institute at Carnegie Mellon University, then tailored to the NASA systems community. This presentation will briefly discuss the six functions for risk management: (1) Identify the risks in a specific format; (2) Analyze the risk probability, impact/severity, and timeframe; (3) Plan the approach; (4) Track the risk through data compilation and analysis; (5) Control and monitor the risk; (6) Communicate and document the process and decisions.

Finally, the presentation will give project managers the information needed to implement Continuous Risk Management successfully at a cost they can afford.

Introduction

Software risk management is important because it helps avoid disasters, rework, and overkill, but more importantly because it stimulates win-win situations. The objectives of software risk management are to identify, address, and eliminate software risk items before they become threats to success or major sources of rework. In general, good project managers are also good managers of risk. It makes good business sense for all software development projects to incorporate risk management as part of project management. NPG 7120.5A, the NASA guidebook for project managers, requires risk management applications and includes a section briefly discussing what should be included in a risk management plan. A course in continuous risk management was developed by the Software Engineering Institute at Carnegie Mellon University and has been adapted to NASA by the Software Assurance Technology Center (SATC) at NASA GSFC. The course was first taught in January, 1998, and has since been taught to over 300 students at all NASA centers.

There are a number of definitions and uses for the term risk, but there is no universally accepted definition. What all definitions have in common is agreement that risk has two characteristics:

uncertainty: An event may or may not happen.

loss: An event has unwanted consequences or losses.

Therefore, risk involves the likelihood that an undesirable event will occur, and the severity of the consequences of the event, should it occur. Risk management can:

- Identify potential problems and deal with them when it is easier and cheaper to do so—before they are problems and before a crisis exists.
- Focus on the project's objective and consciously look for things that may affect quality throughout the production process.
- Allow the early identification of potential problems (the proactive approach) and provide input into management decisions regarding resource allocation.
- Involve personnel at all levels of the project; focus their attention on a shared product vision, and provide a mechanism for achieving it.
- Increase the chances of project success.

At NASA, we focus on Continuous Risk Management that can be applied to any development process: hardware, software, systems, etc. It provides a disciplined environment for proactive decision making to:

- assess continually what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks
- assure, measure effectiveness of the implemented strategies

Risk management must not be allowed to become "shelfware". The process must be a part of regularly scheduled periodic product management. It requires identifying and managing risks routinely throughout all phases of the project's life. The paradigm shown in Figure 1 illustrates the set of continuous risk management functions throughout the life cycle of a project. These functions serve as the foundation for the application of continuous risk management. Each risk nominally goes through these functions sequentially, but the activity occurs continuously, concurrently, and iteratively. Risks are usually tracked in parallel while new risks are identified and analyzed, and the mitigation plan for one risk may yield another risk.

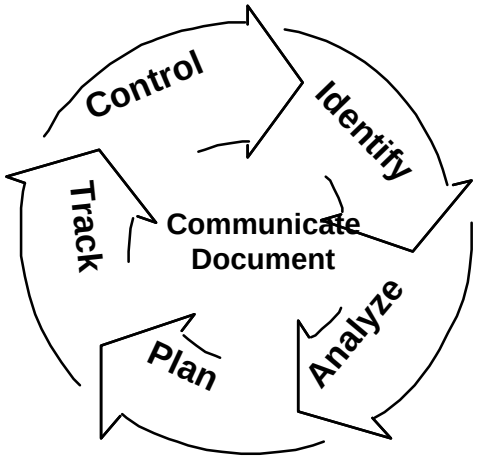

Figure 1: Continuous Risk Management Principle Functions

Continuous Risk Management Principle Functions

1- Identify

The purpose of identification is to consider risks before they become problems and to incorporate this information into the project management process. Anyone in a project can identify risks to the project. Each individual has particular knowledge about various parts of a project. During Identify, uncertainties and issues about the project are transformed into distinct (tangible) risks that can be described and measured.

During this function, all risks are written with the same, two part format. The first part is the risk statement, written as a single statement concisely specifying the cause of the concern as well as its impact. The second part may contain additional supporting details in the form of a context.

The aim for a risk statement is that it be clear, concise, and sufficiently informative that the risk is easily understood. Risk statements in standard format must contain two parts: the condition and the consequence. The condition-consequence format provides a complete picture of the risk, which is critical during mitigation planning. It is read as follows:

*given the <**condition**> there is a possibility that <**consequence**> will occur*

The *condition* component focuses on what is currently causing concern; it must be something that is true or widely perceived to be true. This component provides information that is useful when determining how to mitigate a risk. The *consequence* component focuses on the intermediate and long-term impact of the risk. Understanding the depth and breadth of the impact is useful in determining how much time, resources, and effort should be allocated to the mitigation effort. A well-formed risk statement usually has only one condition, but may have more than one consequence.
Risk statements should avoid:

- abbreviations/acronyms that are not readily understood
- sweeping generalizations
- massive, irrelevant detail

Since the risk statement is to be concise, a context is added to provide enough additional information about the risk to ensure that the original intent of the risk can be understood by other personnel, particularly after time has passed. An effective context captures the what, when, where, how, and why of the risk by describing the circumstances, contributing factors, and related issues (background and additional information that are NOT in the risk statement).

A diagram of the complete risk statement and context are shown in Figure 2.

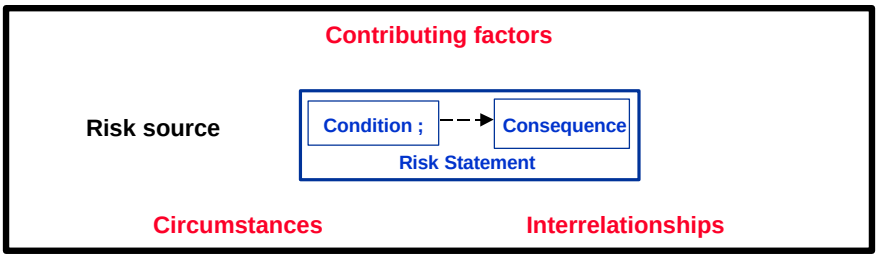

Figure 2: Risk Statement and Context

An example is shown in Figure 3. Note there is one condition and two consequences in the risk statement. The context explains why this is a risk.

Risk statement:

This is the first time that the software staff will use OOD; the staff may have a lower-than-expected productivity rate and schedules may slip because of the associated learning curve.

Context:

Object oriented development is a very different approach that requires special training. There will be a learning curve until the staff is up to speed. The time and resources must be built in for this or the schedule and budget will overrun.

Figure 3: Example Risk Statement and Context

Risk identification depends heavily on both open communication and a forward-looking view to encourage all personnel to bring forward new risks and to plan beyond their immediate problems. Although individual contributions play a role in risk management, teamwork improves the chances of identifying new risks by allowing personnel to combine their knowledge and understanding of the project.

2 - Analyze

The purpose of Analyze is to convert the data into decision-making information. Analysis is a process of examining the risks in detail to determine the extent of the risks, how they relate to each other, and which ones are the most important. Analyzing risks has three basic activities: evaluating the attributes of the risks (impact, probability, and timeframe), classifying the risks, and prioritizing or ranking the risks.

Evaluating - The first step provides better understanding of the risk by qualifying the expected impact, probability, and timeframe of a risk. This involves establishing values for:

Impact: the loss or negative affect on the project should the risk occur
Probability: the likelihood the risk will occur
Timeframe: the period when you must take action in order to mitigate the risk

Figure 4 demonstrates sample values that might be used to evaluate a risk's attributes

Attribute	Value	Description
Probability	Very Likely (H) Probable (M) Improbable (L)	High chance of this risk occurring, thus becoming a problem > 70% Risk like this may turn into a problem once in a while {30% < x < 70%} Not much chance this will become a problem {0% < x < 30%}
Impact	Catastrophic (H)	Loss of system; unrecoverable failure of system operations; major damage to system; schedule slip causing launch date to be missed; cost overrun greater than 50% of budget
	Critical (M)	Minor system damage to system with recoverable operational capacity; cost overrun exceeding 10% (but less than 50% of planned cost
	Marginal (L)	Minor system damage to project; recoverable loss of operational capacity; internal schedule slip that does not impact launch date cost overrun less than 10% of planned cost
Timeframe	Near-term (N) Mid-term (M) Far-term (F)	Within 30 days 1 to 4 months from now more than 4 months from now *NOTE: refers to* ***when action must be taken***

Figure 4: Sample Attribute Values

Classifying - The next step is to classify risks. There are several ways to classify or group risks. The ultimate purpose of classification is to understand the nature of the risks facing the project and to group any related risks so as to build more cost-effective mitigation plans. The process of classifying risks may reveal that two or more risks are equivalent—the statements of risk and context indicate that the subject of these risks is the same. Equivalent risks are therefore duplicate statements of the same risk and should be combined into one risk.

Prioritize - The final step in the Analysis function is to prioritize the risks. The purpose is to sort through a large number of risks and determine which are most important and to separate out which risks should be dealt with first (the vital few risks) when allocating resources. This involves partitioning risks or groups of risks based on the "vital few" sense and ranking risks or sets of risks based on consistently applying an established set of criteria. No project has unlimited resources with which to mitigate risks. Thus, it is essential to determine consistently and efficiently which risks are most important and then to focus those limited resources on mitigating risks.

Conditions and priorities will change during a project, and this natural evolution can affect the important risks to a project–. ***Risk analysis must be a continual process***. Analysis requires open communication so that prioritization and evaluation is accomplished using all known information. A forward-looking view enables personnel to consider long-range impacts of risks.

3 - Plan

Planning is the function of deciding what, if anything, should be done about a risk or set of related risks. In this function decisions and mitigation strategies are developed based on current knowledge of project risks.

The purpose of plan is to:

- make sure the consequences and the sources of the risk are known
- develop effective plans
- plan efficiently (only as much as needed or will be of benefit)
- produce, over time, the correct set of actions that minimize the impacts of risks (cost and schedule) while maximizing opportunity and value
- plan important risks first

Figure 5 indicates the potential approaches to Risk Planning.

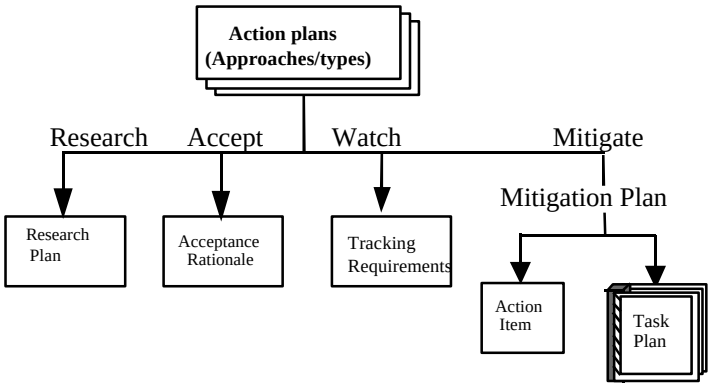

Figure 5: Planning approaches

There are four options to consider when planning for risks:

1. *Research:* establish a plan to research the risk(s)
2. *Accept:* decide to "accept" the risk(s) and document the rationale behind the decision
3. *Watch:* monitor risk conditions for any indications of change in probability or impact (tracking metrics must be established and documented)
4. *Mitigate:* allocate resources and assign actions in order to reduce the probability or potential impact of risks. This can range from simple tasking to sweeping activities:
   Action Items: a series of discrete tasks to mitigate risk
   Task Plan: formal, well-documented and larger in scope

Dealing with risk is a continuous process of determining what to do with new concerns as they are identified and efficiently utilizing project resources. An integrated approach to management is needed to ensure mitigation actions do not conflict with project or team plans and goals. A shared product vision and global perspective are needed to create mitigation actions on the macro level to the benefit the project, customer and organization. The focus of risk planning is to be forward looking, to prevent risks from becoming problems. Teamwork and open communication enhance the planning process by increasing the amount of knowledge and expertise that can be applied to the development of mitigating actions.

4 - Track

Tracking is the process by which risk status data are acquired, compiled, and reported

The purpose of Track is to collect accurate, timely, and relevant risk information and to present it in a clear and easily understood manner to the appropriate people/group. Tracking is done by those responsible for monitoring "watched" or "mitigated" risks. Tracking status information become critical to performing the next function in the Continuous Risk Management paradigm, i.e. Control. Supporting information, such as schedule and budget variances, critical path changes, and project/performance indicators can be used as triggers, thresholds, and risk- or plan-specific measures where appropriate.

When a mitigation plan has been developed for a risk or risk set, both the mitigation plan and the risk attributes are tracked. Tracking the mitigation plan, or even a list of action items, will indicate whether the plan is being executed correctly and/or on schedule. Tracking any changes in the risk attributes will indicate whether the mitigation plan is reducing the impact or probability of the risk. In other words, tracking risk attributes gives an indication of how effective the mitigation plan is.

Program and risk metrics provide decision makers with the information needed for making effective decisions. Normally program metrics are used to assess the cost and schedule of a program as well as the performance and quality of a product. Risk metrics are used to measure a risk's attributes and assess the progress of a mitigation plan. They can also be used to help identify new risks.

> *Example*: A program metric might look at the rate of module completion. If this metric indicates that the rate of completion is lower than expected, then a schedule risk should be identified.

Open communication regarding risk and mitigation status stimulates the project and risk management process. Tracking is a continuous process - current information about a risk status should be conveyed regularly to the rest of the project. Risk metrics provide decision makers with the information needed for making effective decisions.

5 - Control

The purpose of the Control function is to make informed, timely, and effective decisions regarding risks and their mitigation plans. It is the process that takes in tracking status information and decides exactly what to do based on the reported data. Controlling risks involves analyzing the status reports, deciding how to proceed, and then implementing those decisions.

Decision makers need to know 1) when or whether there is a significant change in risk attributes and 2) the effectiveness of mitigation plans within the context of project needs and constraints. The goal is to obtain a clear understanding of the current status of each risk and mitigation plan relative to the project and then to make decisions based on that understanding. Tracking data is used to ensure that project risks continue to be managed effectively and to determine how to proceed with project risks. Options include:

- *Replan* - A new or modified plan is required when the threshold value has been exceeded, analysis of the indicators shows that the action plan is not working, or an unexpected adverse trend is discovered.

- *Close the risk* - A closed risk is one that no longer exists or is no longer cost effective to track as a risk. This occurs when: the probability falls below a defined threshold, impact lies below a defined threshold, or the risk has become a problem and is tracked.
- *Invoke a contingency plan* - A contingency plan is invoked when a trigger has been exceeded or some other related action needs to be taken.
- *Continue tracking and executing the current plan* - No additional action is taken when analysis of the tracking data indicates that all is going as expected or project personnel decide to continue tracking the risk or mitigation plan as before.

Open communication is important for effective feedback and decision making - a critical aspect of Control. Risk control is also enhanced through integrated management - combining it with routine project management activities enables comprehensive project decision making.

6 - Communication & Documentation

The purpose of Communicate and Document is for *all* personnel to understand the project's risks and mitigation alternatives as well as risk data and to make effective choices within the constraints of the project. Communication and Documentation are essential to the success of all other functions within the paradigm and is critical for managing risks.

Identify: In risk identification, risk statements are communicated.

Analyze: In analysis, project personnel communicate information about impact, probability, and timeframe attributes. Risk classification involves grouping risk information communicated by individuals.

Plan: During planning, action plans are developed and communicated to project personnel.

Track: Reports designed to communicate data to decision-makers are compiled during tracking.

Control: The decisions made during control must be communicated and recorded to project personnel.

For effective risk management, an organization must have open communication and formal documentation. Communication of risk information is often difficult because the concept of risk comprises two subjects that people don't normally deal well with: probability and negative consequences.

Not only Continuous Risk Management, but the project as a whole are in jeopardy when the environment is not based on open communication. No one has better insight into risks than project personnel, and *management needs that input*. Experienced managers know that the free flow of information can make or break any project. Open communication requires:

- Encouraging free-flowing information at and between all project levels
- Enabling forma, informal and impromptu communication
- Using consensus-based processes that value the individual voice, bringing unique knowledge and insight to identifying and managing risks.

NASA Risk Management Course

Risk is a daily reality on all projects, and Continuous Risk Management should become just as routine. It should be ongoing and comfortable and neither imposed nor forgotten. Like any good habit, it should seamlessly fit into the daily work. During the course taught at NASA, various tools and methods are demonstrated that will work for any project. The key is to adhere to the principles, perform the functions, and adapt the practice to fit the project's needs. Continuous risk management is not "one size fits all". To be effective, tailoring is needed. Tailoring occurs when organizations adapt the processes, select methods and tools which best fit their project management practice and their organizational culture. Following the principles of the continuous risk management is the key to successful tailoring.

With this in mind, the Continuous Risk Management course for NASA was tailored to 2 days. The first day is lecture, covering all material with some exercises applying the methods and tools. This is a very intense day since there is a lot of information to absorb. The second day is devoted to a "project" workshop. In most classes, personnel from one or two projects attend the lecture then split for the workshop (Classes are limited to 20 students.) The workshop is done in small groups, periodically these groups come together to review what each group has chosen to work on. (It is interesting as the instructor to observe the similarities in their results.) Depending on the audience, there are two possible workshops, one for management and the other for the implementation team.

The workshop for management starts by compiling the project information needed for the risk management plan. This starts with getting the functional organizational chart, identifying key meetings where risk management activities should take place, and identifying key personnel. The methods and tools to be used are then selected, and the criteria for the attributes probability, impact and timeframe are defined. This usually takes 2-3 hours. A shortened version of the implementation workshop described below is then applied.

The implementation workshop starts by identifying risks to the project based on everyone's knowledge. Phrases are used, with brainstorming to get a list of over 20 potential risks. It is stressed that if it is a problem now, it is not a risk. From this list 5 risks are identified as those the group feels they can do something about and would like to work on. The risks are then written using the correct format of condition and consequence. The risk context is discussed but not written. Using these 5 risks and the attribute definitions from management, the risks are classified and prioritized. A mitigation plan for the top risk is developed, data for tracking is identified and presentation formats discussed. Depending on time, 2 or 3 risks are processed through this cycle so that the attendees not only feel comfortable with the process, they have some risks specific to their project that they can start working on. Based on course feedback, it is believed the workshop is the key to the success of this training.

When a class is not all from the same project, either the group is told to make up a project based on common experience, or use a project that many of them are familiar with. The

second option is encouraged so real work is actually accomplished although it only benefits a few of the attendees.

After completion of the course, students should:

- Understand the concepts and principles of Continuous Risk Management and how to apply them
- Possess basic risk management skills for each function of the risk management paradigm
- Be able to use the key methods and tools
- Be able to tailor CRM to a project or organization

Implementation

Three steps should be considered by projects when implementing risk management. First, project risk management should be arranged. The training in itself is not important, it is what the training does for the project. The training helps the project to see how a formal process can be used to manage risks, but more importantly facilitate communication and initial brainstorming among project personnel. Second, the project should adopt tools that they are familiar with to aid in the tracking of risks and communication of risk status. The key is that the project use tools that they know how to use and that they *will use*. Lastly, the risk management process needs to be integrated into the normal project management process. Risk management must become the normal way of doing project business. This will ensure that rather than a separate process requiring extra overhead, risk management is ingrained in the project. This will lead to a cost-effective implementation within the project.

Conclusion

Most project managers agree that risk management works, but the difficulty lies in actually implementing it, even when required to do so. The risk management plan is often hastily written and then thrown in a corner to gather dust. In addition to the course, one of the steps NASA has taken is to establish a risk management web site (http://satc.gsfc.nasa.gov) that contains sample risk management plans and a schedule of classes. Much time is spent discussing with managers the benefits of taking a formal training course, which is more than recovered by a project when all team members are working toward common goals in a coordinated manner.

"Continuous Risk Management at NASA" was presented at the Applied Software Measurement / Software Management Conference, February 1999, San Jose, California.